

- 10 -

REMARKS

The Examiner has stated that applicant's arguments have been fully considered but are not persuasive. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of multiple dependent claims into each of the independent claims. Since the subject matter of such dependent claims was already considered by the Examiner, it is asserted that such claim amendments would not require new search and/or consideration.

The Examiner has rejected Claims 1-37 under 35 U.S.C. 103(a) as being unpatentable over Hodges (U.S. Patent No. 6,269,456) in view of Van Huben et al. (U.S. Patent No. 6,237,594). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on Figures 4 and 7 along with the following excerpts from Hodges to make a prior art showing of applicant's claimed, "whereby the central service computer and the user computer are each configured to send the new antivirus file to the other of the central service computer and the user computer to update the antivirus database" (see this or similar, but not identical, language in each of the foregoing claims):

"Using means not shown in FIG. 3, central antivirus server 308 is kept up-to-date with the latest releases of antivirus files..."  
(Col. 7, lines 1-3)

"At step 410 antivirus update files are received by client computer 302 if any such files are sent by the central antivirus server 308. If any such files are received, at step 412 the antivirus update files are loaded. If any such files are not received, at step 414 the antivirus update agent pauses for a period of time. Following step 412 or 414, as the case may be, the decision step 406 is again performed if the client computer is still turned on and operating, as reflected by a positive branch at step 416. The loading step shown at FIG. 4 may be an automatic loading step, wherein the downloaded files

- 11 -

automatically self-execute and insert the updated file VIRUS\_SIGNATURES.DAT into the appropriate directory of the client computer 302. Optionally, according to another preferred embodiment, the downloaded file may cause a "flash" notification to be seen by the user, advising the user that new antivirus files have been downloaded, and that the existing files currently being used in the antivirus application are now outdated. The user may then be given the option to (a) allow the downloaded files to be extracted and installed immediately, or (b) obey the installation process until a later time." (Col. 7, lines 45-63-emphasis added)

"At step 614, central antivirus server 308 then updates the subscriber database to reflect that user BJONES001234 has received the updated antivirus file." (Col. 9, lines 53-55-emphasis added)

"FIG. 7 shows a diagram of a database 700 contained within central antivirus server 308. Database 700 comprises an antivirus database 702 and a subscriber database 704 as shown in FIG. 7. Shown in antivirus database 702 are virus signature files and executable program files which represent the latest available versions..." (Col. 9, lines 62-67)

Applicant respectfully asserts that such excerpts merely teach antivirus update files that are received by a client computer and a central antivirus server that is kept up-to-date with antivirus files (see emphasized excerpts above). However, a general teaching of a central antivirus server that is kept up-to-date, as in Hodges, does not meet applicant's specific claim language. In particular, applicant claims "whereby the central service computer and the user computer are each configured to send the new antivirus file to the other of the central service computer and the user computer to update the antivirus database" (emphasis added). Applicant emphasizes that simply teaching that a central antivirus server is kept up-to-date, as in Hodges, does not meet any sort of "user computer [that is] configured to send the new antivirus file to the...central service computer," as claimed by applicant.

In the Examiner's latest arguments, the Examiner states that applicant's claim language is generally a standard feature available in commercial antivirus products such as McAfee VirusScan 4.5. The Examiner argues that McAfee provides features which allow for the detection of new viruses at the local computer level along with DAT file updates. The Examiner concludes that "a skilled artisan would have known to use the McAfee configuration features to realize the claimed elements relating to configuring a

central computer and user computer to send new antivirus files to other central computers and user computers in updating the antivirus database.”

Applicant respectfully asserts that merely teaching the detection of new viruses at a local computer, as the Examiner asserts McAfee teaches, does not meet any sort of user computer that is “configured to send the new antivirus file to...the central service computer...to update the antivirus database,” as claimed by applicant. Simply because a local computer may be able to detect new viruses, does not inherently or otherwise also include the capability of “send[ing a] new antivirus file to...[a] central service computer...to update the antivirus database,” and especially not when read in the context of applicant’s claim language where “the user computer and the central service computer each [have] an antivirus database” (see the preamble of each of the independent claims).

In addition, the Examiner has again relied on McAfee’s teaching of detecting new viruses at a local computer level to meet applicant’s claimed “wherein the user computer is configured to send the new antivirus file to the central service computer to update the virus database, if is determined that the user computer contains the new antivirus file not contained within the central service computer” (see this or similar, but not identical, language in each of the foregoing claims). For substantially the same reasons as argued above, applicant respectfully asserts that neither the Hodges nor Van Huben references teach such specific claim language. In addition, such claim language does not generally constitute standard features available in commercial antivirus products, as the Examiner argues.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the

- 13 -

prior art and not based on applicant's disclosure. *In re Vaack*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has included the subject matter of Claims 4, 7 and 33 into each of the independent claims.

With respect to the subject matter of Claim 4, the Examiner has relied on the excerpts cited above with respect to the independent claims to make a prior art showing of applicant's claimed technique "wherein the central service computer is configured to periodically obtain updated antivirus files from the antivirus server." Applicant respectfully asserts that such excerpts do not teach a central service computer in the context claimed by applicant. Specifically, Hodges only generally teaches a "central antivirus server 308 [that] is kept up-to-date" (see Col. 7, lines 1-3). Applicant also notes that Hodges teaches a "push administration system 810 [that] pushes channelized information to the client desktop 802" (see Col. 10, lines 50-51-emphasis added). Thus, Hodges clearly does not teach that "a central service computer is configured to periodically obtain updated antivirus files from the antivirus server," as claimed by applicant (emphasis added).

With respect to the subject matter of Claims 7 and 33, the Examiner has relied on Col. 9, lines 53-55 and 62-67 along with Figure 7 to make a prior art showing of applicant's claimed "notifying the central service computer of the new antivirus data file located on the user computer, and the user computer inquiring whether to update the antivirus database with new antivirus files" (Claim 7) and claimed technique "wherein after the central service computer is notified of the new antivirus data file located on the user computer, the user computer waits for a request from the central service computer to send the new antivirus data file" (Claim 33).

- 14 -

However, the Examiner has stated that "Hodges teaches notifying [the] server of user update requirements." Applicant respectfully asserts that simply notifying a server of user update requirements does not meet applicant's specific claim language, namely "notifying the central service computer of the new antivirus data file located on the user computer" (Claim 7-emphasis added) and that "the central service computer [is notified] of the new antivirus data file located on the user computer" (Claim 33-emphasis added), so that the user computer waits for a request from the central service computer to send the new antivirus data file.

Since at least the third element of the prima facie case of obviousness has not been met, as noted above, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P313/01.051.02).

Respectfully submitted,  
Zilka-Kotab, PC.

Kevin J. Zilka  
Registration No. 41,429

P.O. Box 721120  
San Jose, CA 95172-1120  
408-505-5100